

USER AUTHENTICATION SYSTEM

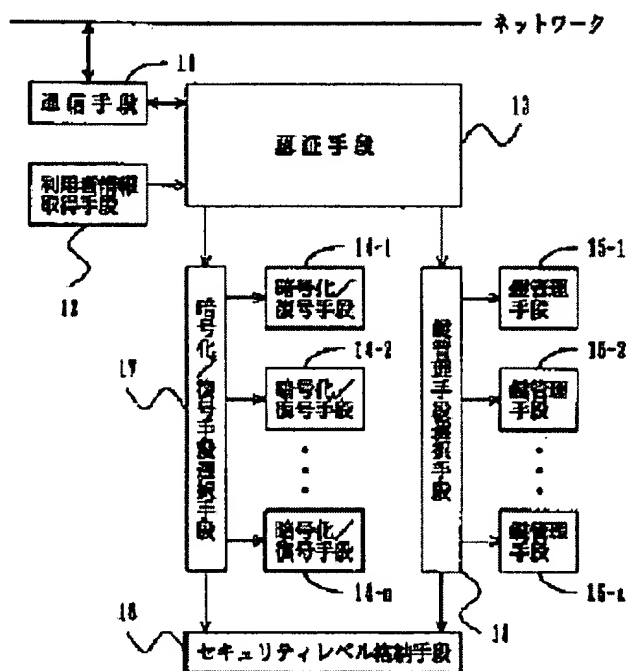
Patent number: JP8297638
Publication date: 1996-11-12
Inventor: SUGIYAMA HIROYUKI; TANABE KATSUHIRO
Applicant: NIPPON TELEGR & TELEPH CORP <NTT>
Classification:
 - international: G06F15/00; G06F13/00; G09C1/00; H04L9/00; H04L9/10; H04L9/12
 - european:
Application number: JP19950102521 19950426
Priority number(s):

Report a data error here

Abstract of JP8297638

PURPOSE: To provide the user authentication system which can select any ciphering/deciphering means or a key managing means at different security levels suitable for the request of a user or terminal equipment.

CONSTITUTION: This system is provided with plural ciphering/deciphering means from 14-1 to 14-m corresponding to different security levels, plural key managing means from 15-1 to 15-n corresponding to different security levels, security level storage means 16 for storing the security level for each user or terminal equipment designated in advance, ciphering/deciphering means selecting means 17 for selecting the ciphering/deciphering means from 14-1 to 14-m corresponding to the security levels at the time of ciphering/deciphering processing, and key managing means selecting means 18 for selecting the key managing means from 15-1 to 15-n corresponding to the security levels at the time of key acquisition. Thus, ciphering/deciphering processing or key management suitable for the request of the user or terminal equipment is performed.



Data supplied from the esp@cenet database - Patent Abstracts of Japan

(51) Int.Cl. ⁶	識別記号	庁内整理番号	F I	技術表示箇所
G 0 6 F 15/00	3 3 0	9364-5L	G 0 6 F 15/00	3 3 0 D
	13/00	3 5 7		3 5 7 Z
G 0 9 C 1/00		7259-5J	G 0 9 C 1/00	
H 0 4 L 9/00			G 0 6 F 1/00	3 7 0 E
9/10			H 0 4 L 9/00	Z

審査請求 未請求 請求項の数 2 O L (全 6 頁) 最終頁に続く

(21) 出願番号 特願平7-102521

(22) 出願日 平成7年(1995)4月26日

(71) 出願人 000004226

日本電信電話株式会社

東京都新宿区西新宿三丁目19番2号

(72) 発明者 杉山 広幸

東京都千代田区内幸町1丁目1番6号 日

本電信電話株式会社内

(72) 発明者 田辺 克弘

東京都千代田区内幸町1丁目1番6号 日

本電信電話株式会社内

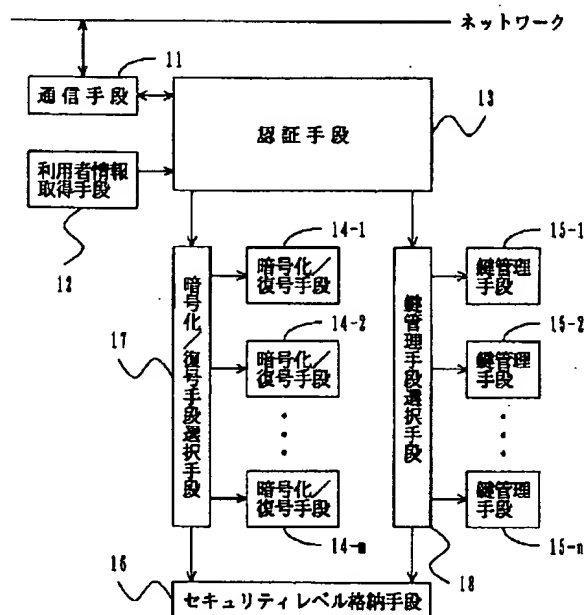
(74) 代理人 弁理士 吉田 精孝

(54) 【発明の名称】 利用者認証方式

(57) 【要約】

【目的】 利用者や端末装置の要求に適したセキュリティレベルの異なる暗号化／復号手段又は鍵管理手段を選択可能な利用者認証方式を提供する。

【構成】 異なるセキュリティレベルに応じた複数の暗号化／復号手段14-1～14-mと、異なるセキュリティレベルに応じた複数の鍵管理手段15-1～15-nと、予め指定された利用者や端末装置毎のセキュリティレベルを格納するセキュリティレベル格納手段16と、暗号化／復号処理時にセキュリティレベルに対応した暗号化／復号手段を選択する暗号化／復号手段選択手段17と、鍵取得時にセキュリティレベルに対応した鍵管理手段を選択する鍵管理手段選択手段18とを備えたことにより、利用者や端末装置の要求に適した暗号化／復号処理、鍵管理を行う。



【特許請求の範囲】

【請求項1】 利用者の指示に従ってサービスを要求する端末装置と、サービスを提供するサーバと、これらを接続するネットワークとを備えたクライアントサーバ型分散ネットワークシステムにおける前記利用者がサーバに対してサービスを要求する資格を備えた正規の利用者であることを認証する利用者認証方式において、異なるセキュリティレベルに応じた暗号化／復号処理をそれぞれ実行する複数の暗号化／復号手段と、予め指定された利用者や端末装置毎のセキュリティレベルを格納するセキュリティレベル格納手段と、暗号化／復号処理時に複数の暗号化／復号手段からセキュリティレベル格納手段に格納されたセキュリティレベルに対応した暗号化／復号手段を選択する暗号化／復号手段選択手段とを備えたことを特徴とする利用者認証方式。

【請求項2】 利用者の指示に従ってサービスを要求する端末装置と、サービスを提供するサーバと、これらを接続するネットワークとを備えたクライアントサーバ型分散ネットワークシステムにおける前記利用者がサーバに対してサービスを要求する資格を備えた正規の利用者であることを認証する利用者認証方式において、異なるセキュリティレベルに応じた鍵管理をそれぞれ実行する複数の鍵管理手段と、予め指定された利用者や端末装置毎のセキュリティレベルを格納するセキュリティレベル格納手段と、鍵取得時に複数の鍵管理手段からセキュリティレベル格納手段に格納されたセキュリティレベルに対応した鍵管理手段を選択する鍵管理手段選択手段とを備えたことを特徴とする利用者認証方式。

【発明の詳細な説明】

【0001】

【産業上の利用分野】 本発明は、クライアントサーバ型分散ネットワークシステムにおける利用者認証方式に関するものである。

【0002】

【従来の技術】 従来、クライアントサーバ型分散ネットワークシステムにおける認証方式としては、MITのAthenaプロジェクトによって開発されたKerberosが広く知られている（Jennifer G. Steiner, Clifford Neuman, Jeffrey I. Schiller, “Kerberos: An Authentication Service for Open Network systems” USENIX Winter Conference, February 9-12, 1988, Dallas, Texas, 又はJohn T. Kohl, “The Evolution of Kerberos Authentication Service” Spring, 1991, EurOpen Conference, Tromso, Norway参照）。

【0003】 Kerberosでは、暗号アルゴリズムとしてDESを採用した、信頼できる第三者に基づく利用者認証機能を提供している。まず、Kerberosにおける利用者認証方式について説明する。

【0004】 図1はクライアントサーバ型分散ネットワークシステムの概要を示すもので、図中、1は利用者の指示に従ってサービスを要求するクライアントコンピュータ（以下、端末装置と称す。）、2はサービスを提供するサーバコンピュータ（以下、単にサーバと称す。）、3はサーバ2に対して端末装置1の利用者が正規の利用者（サーバに対してサービスを要求する資格を備えた利用者）であることを認証する認証サーバコンピュータ（以下、単に認証サーバと称す。）、4は端末装置1、サーバ2及び認証サーバ3を接続するネットワークである。

【0005】 Kerberosにおける利用者認証方式では、端末装置1は利用者から指定されたパスワードよりDESの鍵である利用者の秘密鍵Kuを生成する手段と、メッセージをDESアルゴリズムに従って暗号化／復号する手段と、時刻を取得する手段とを有し、サーバ2はサーバ自身であることを示すDESの鍵であるサーバの秘密鍵Ksを保持する手段と、メッセージをDESアルゴリズムに従って暗号化／復号する手段と、時刻を取得する手段とを有し、認証サーバ3はDESの鍵である利用者の秘密鍵Ku及びサーバ2の秘密鍵Ksの両者を保持する手段と、端末装置1及びサーバ2で共有されるDESの鍵であるセッション鍵を生成する手段とを有している。

【0006】 以下、Kerberosにおける利用者認証方式をステップ毎に説明するが、この際、 $E(Kx, X)$ はXを鍵Kxで暗号化した値、 $D(Kx, X)$ はXを鍵Kxで復号した値、また、 $X \parallel Y$ はXとYとを連結した値をそれぞれ示すものとする。

【0007】（ステップ1） 利用者の指示に基づいて端末装置1はネットワーク4を経由して認証サーバ3に、サーバ2に対して利用者が正規の利用者であることを証明するために用いるセッション鍵Kusを要求する。

【0008】（ステップ2） 認証サーバ3は、端末装置1からの要求が該認証サーバ3がその秘密鍵を保持している利用者の指示に基づくものであれば、セッション鍵Kusを生成し、これを該利用者の秘密鍵KuでDESアルゴリズムに従って暗号化するとともに、該セッション鍵Kusをサーバ2の秘密鍵KsでもDESアルゴリズムに従って暗号化し、端末装置1にネットワーク4を経由してこれらの暗号化されたセッション鍵 $E(Ku, Kus)$ 、 $E(Ks, Kus)$ を送る。

【0009】（ステップ3） 端末装置1は認証サーバ3からネットワーク4を経由して送られてきた、利用者の秘密鍵Kuで暗号化されたセッション鍵 $E(Ku, Kus)$ を、利用者から入力されたパスワードより生成した該利用者の秘密鍵KuでDESアルゴリズムに従って復号し、サーバ2とのセッション鍵Kusを得る。

【0010】（ステップ4） 端末装置1は現在の時刻T1を取得し、これをセッション鍵KusでDESアルゴ

リズムに従って暗号化し、認証サーバ3から受け取った前記セッション鍵E (Ks, Kus) とともにネットワーク4を経由してサーバ2に送る。

【0011】(ステップ5) サーバ2は受け取った前記セッション鍵E (Ks, Kus) を、自身の秘密鍵KsでDESアルゴリズムに従って復号してセッション鍵Kusを得る。このセッション鍵Kusで端末装置1から送られた、暗号化された時刻E (Kus, T1) をDESアルゴリズムに従って復号し、時刻T1を得る。

【0012】そして、現在の時刻T2を取得し、時刻T1と時刻T2とを比較し、T1 + 5分 < T2であれば、端末装置1にサービスの要求を指示した利用者は正規の利用者であると判断してサービスの提供を開始し、そうでなければ正規の利用者ではないと判断してサービスの提供を拒否する。

【0013】

【発明が解決しようとする課題】このようにKerberosでは、利用者認証の過程において常にDESアルゴリズムに従って暗号化／復号を行い、他の異なる暗号アルゴリズムを選択することはできない。しかしながら、実際のシステムにおいてはその形態や提供するサービス等の条件により、個々の利用者や端末装置毎にセキュリティレベル(安全性)の異なる利用者認証方式を採用したい場合がある。

【0014】例えば、社内の掲示板サービスの場合にはセキュリティレベルが低くてもレスポンスタイムを優先した利用者認証方式を採用したいが、人事システムの場合にはセキュリティレベルが非常に高い利用者認証方式を採用したいという要求がある。この際、掲示板サービスでの利用者認証に用いる暗号アルゴリズムはFEAL-8のCBCモードを、人事システムでの利用者認証に用いる暗号アルゴリズムはFEAL-32XのCBCモードをというように、要求されるセキュリティレベルに適した暗号アルゴリズムを、同一のシステム内で個々の利用者や端末装置毎に選択できることが望まれる。

【0015】また同様に、利用者のアイデンティティを示す秘密鍵を管理する手段も、Kerberosでは利用者が記憶したパスワードから自動的に生成する手段のみしか持たず、ハッカーらのパスワードアタックに対しては従来のパスワード入力方式の利用者認証方式と同じ程度の安全性しか提供することができない。

【0016】しかしながら、現在ではICカード等の極めて安全性の高い装置を利用可能であり、高いセキュリティレベルが要求される場合はコストがかかってもこのような装置を用い、それほどのセキュリティが要求されない場合はKerberosと同様なパスワードから自動的に生成する手段を用いるというように、要求されるセキュリティレベルに適した秘密鍵の管理手段を、同一のシステム内で個々の利用者や端末装置毎に選択できることが望まれる。

【0017】本発明の目的は、利用者や端末装置の要求に適したセキュリティレベルの異なる暗号化／復号手段を同一のシステム内で選択可能な利用者認証方式を提供することにある。

【0018】本発明の他の目的は、利用者や端末装置の要求に適したセキュリティレベルの異なる秘密鍵の管理手段を同一のシステム内で選択可能な利用者認証方式を提供することにある。

【0019】

【課題を解決するための手段】本発明では前記目的を達成するため、請求項1では、利用者の指示に従ってサービスを要求する端末装置と、サービスを提供するサーバと、これらを接続するネットワークとを備えたクライアントサーバ型分散ネットワークシステムにおける前記利用者がサーバに対してサービスを要求する資格を備えた正規の利用者であることを認証する利用者認証方式において、異なるセキュリティレベルに応じた暗号化／復号処理をそれぞれ実行する複数の暗号化／復号手段と、予め指定された利用者や端末装置毎のセキュリティレベルを格納するセキュリティレベル格納手段と、暗号化／復号処理時に複数の暗号化／復号手段からセキュリティレベル格納手段に格納されたセキュリティレベルに対応した暗号化／復号手段を選択する暗号化／復号手段選択手段とを備えた利用者認証方式を提案する。

【0020】また、請求項2では、利用者の指示に従ってサービスを要求する端末装置と、サービスを提供するサーバと、これらを接続するネットワークとを備えたクライアントサーバ型分散ネットワークシステムにおける前記利用者がサーバに対してサービスを要求する資格を備えた正規の利用者であることを認証する利用者認証方式において、異なるセキュリティレベルに応じた鍵管理をそれぞれ実行する複数の鍵管理手段と、予め指定された利用者や端末装置毎のセキュリティレベルを格納するセキュリティレベル格納手段と、鍵取得時に複数の鍵管理手段からセキュリティレベル格納手段に格納されたセキュリティレベルに対応した鍵管理手段を選択する鍵管理手段選択手段とを備えた利用者認証方式を提案する。

【0021】

【作用】本発明の請求項1によれば、利用者の認証に伴って該利用者の秘密鍵を用いた暗号／復号化処理を行う際、複数の暗号化／復号手段から暗号化／復号手段選択手段により、セキュリティレベル格納手段に格納された利用者や端末装置毎のセキュリティレベルに対応した暗号化／復号手段を選択することができ、利用者や端末装置毎のセキュリティレベルに応じた利用者の認証を行うことができる。

【0022】また、請求項2によれば、利用者の認証に伴って該利用者の秘密鍵を取得する際、複数の鍵管理手段から鍵管理手段選択手段により、セキュリティレベル格納手段に格納された利用者や端末装置毎のセキュリテ

イレベルに対応した鍵管理手段を選択することができ、利用者や端末装置毎のセキュリティレベルに応じた利用者の認証を行うことができる。

【0023】

【実施例】以下、図面を用いて本発明の実施例を説明するが、ここではISO/IEC 9798-2 “Information technology - Security techniques - Entity authentication mechanisms ; Part 2; Entity authentication using symmetric techniques” の “6.2 Five pass authentication” に示される慣用鍵暗号アルゴリズムに基づく信頼できる第三者を用いた5パス認証方式に本発明を適応した例を示す。

【0024】本実施例におけるクライアントサーバ型分散ネットワークシステムの概要は図1に示したものと同様である。

【0025】図2は本実施例における端末装置を示すもので、図中、11は通信手段、12は利用者情報取得手段、13は認証手段、14-1、14-2、……14-mは暗号化/復号手段、15-1、15-2、……15-nは鍵管理手段、16はセキュリティレベル格納手段、17は暗号化/復号手段選択手段、18は鍵管理手段選択手段である。

【0026】通信手段11はネットワーク4に接続され、サーバ2及び認証サーバ3と通信を行う。利用者情報取得手段12は利用者から利用者識別子を取得する。認証手段13は前記ISO 9798-2に基づく認証方式を実施する。

【0027】暗号化/復号手段14-1～14-mは異なるセキュリティレベルに応じた暗号化/復号処理をそれぞれ実行するもので、FEAL、DES等の各種の異なるアルゴリズムや、EBCモード、CBCモード、CFBモード、OFBモード等の暗号アルゴリズムの各種の異なる利用モードを備えている。鍵管理手段15-1～15-nは異なるセキュリティレベルに応じた秘密鍵の管理を実行するもので、ICカードやPCMCIAカード、ROM等の各種の異なるハードウェアを備えている。

【0028】セキュリティレベル格納手段16は予め指定された利用者や端末装置毎のセキュリティレベルを格納する。暗号化/復号手段選択手段17は暗号化/復号手段14-1～14-mのうち、セキュリティレベル格納手段16に格納されているセキュリティレベルに対応したものを認証手段13からの要求に基づいて選択する。鍵管理手段選択手段18は鍵管理手段15-1～15-nのうち、セキュリティレベル格納手段16に格納されているセキュリティレベルに対応したものを認証手段13からの要求に基づいて選択する。

【0029】図3は本実施例における端末装置1、サーバ2及び認証サーバ3間でやりとりされるメッセージのシーケンスを示すもので、以下、本実施例における認証

動作を説明する。

【0030】まず、端末装置1は、利用者情報取得手段12を用いて利用者の識別子IDuを取得する。次に、認証手段13にその利用者識別子IDuを渡し、認証手段13はその利用者識別子IDuと生成した乱数RuからメッセージM1を作成し、通信手段11を介してサーバ2に送る。

【0031】サーバ2は、サーバの識別子IDsと生成した乱数Rs1とメッセージM1中のIDu、RuからメッセージM2を作成し、認証サーバ3に送る。

【0032】認証サーバ3は、利用者識別子IDu、サーバ識別子IDsから各々の登録されている秘密鍵Ku、Ksを取得し、さらに端末装置1とサーバ2で共有するセッション鍵Ksuを生成する。次に、このセッション鍵Ksuと端末装置1から送られてきた乱数Ru、サーバ2から送られてきた乱数Rs1を各々連結し、さらに利用者の秘密鍵Ku、サーバ2の秘密鍵Ksでそれらを各々暗号化し、メッセージM3、即ちE(Ku, Ru || Ksu)、E(Ks, Rs1 || Ksu)を作成し、サーバ2へ送り返す。

【0033】サーバ2は、メッセージM3の一部であるE(Ks, Rs1 || Ksu)を、サーバ2の秘密鍵Ksで復号し、乱数Rs1、セッション鍵Ksuを取得する。ここで取得した乱数とメッセージM2で送った乱数とを照合し、一致すればメッセージM3を正しい認証サーバ3からの応答であると判断し、以後の動作を継続する。

【0034】次に、サーバ2は、新たな乱数Rs2を生成し、端末装置1からメッセージM1で送られてきた乱数Ruと連結し、セッション鍵Ksuで暗号化し、メッセージM3の残りの部分とともにメッセージM4、即ちE(Ku, Ru || Ksu)、E(Ksu, Ru || Rs2)を作成し、端末装置1へ送る。

【0035】端末装置1は、メッセージM4を通信手段11で受け取り、認証手段13に渡す。認証手段13はメッセージM4の認証サーバ3から送られてきた部分E(Ku, Ru || Ksu)を復号するために、まず、鍵管理手段選択手段18に利用者の秘密鍵Kuの取得を要求する。

【0036】鍵管理手段選択手段18はセキュリティレベル格納手段16にセキュリティレベルを問い合わせる。セキュリティレベル格納手段16は、自身が格納しているセキュリティレベルを鍵管理手段選択手段18に伝える。鍵管理手段選択手段18はセキュリティレベル格納手段16から知らされたセキュリティレベルに従って、鍵管理手段15-1～15-nの中から適切な鍵管理手段を選択し、その鍵管理手段を用いて利用者の秘密鍵Kuを取得し、認証手段13に渡す。

【0037】次に、認証手段13は暗号化/復号手段選択手段17に、鍵管理手段選択手段18から得た利用者の秘密鍵KuによるE(Ku, Ru || Ksu)の復号を要

求する。暗号化／復号手段選択手段17はセキュリティレベル格納手段16にセキュリティレベルを問い合わせる。セキュリティレベル格納手段16は、自身が格納しているセキュリティレベルを暗号化／復号手段選択手段17に伝える。

【0038】暗号化／復号手段選択手段17は、セキュリティレベル格納手段16から知らされたセキュリティレベルに従って、暗号化／復号手段14-1～14-mの中から適切な暗号化／復号手段を選択し、その暗号化／復号手段を用いて $E(K_u, R_u \parallel K_{su})$ の復号を行い、乱数 R_u 、セッション鍵 K_{us} を取得し、認証手段13に渡す。

【0039】認証手段13は、暗号化／復号手段選択手段17から取得した乱数とメッセージM1で送った乱数とを照合し、一致すればメッセージM4を正しい認証サーバからの応答であると判断し、以後の動作を継続する。

【0040】次に、得られたセッション鍵 K_{us} でメッセージM4の認証サーバ3から送られてきた部分 $E(K_s, R_u \parallel R_{s2})$ の復号を暗号化／復号手段選択手段17に要求する。暗号化／復号手段選択手段17はセキュリティレベル格納手段16にセキュリティレベルを問い合わせる。セキュリティレベル格納手段16は、自身が格納しているセキュリティレベルを暗号化／復号手段選択手段17に伝える。

【0041】暗号化／復号手段選択手段17は、セキュリティレベル格納手段16から知らされたセキュリティレベルに従って、暗号化／復号手段14-1～14-mの中から適切な暗号化／復号手段を選択し、その暗号化／復号手段を用いて $E(K_{su}, R_u \parallel R_{s2})$ の復号を行い、乱数 R_u 、乱数 R_{s2} を取得し、認証手段13に渡す。

【0042】認証手段13は、暗号化／復号手段選択手段17から取得した乱数 R_u と、メッセージM1で送った乱数とを照合し、一致すればメッセージM4を正しいサーバ2からの応答であると判断し、以後の動作を継続する。

【0043】次に、認証手段13は、得られたセッション鍵 K_{us} でサーバ2から送られてきた乱数 R_{s2} と乱数 R_u の暗号化を、暗号化／復号手段選択手段17に要求する。暗号化／復号手段選択手段17はセキュリティレベル格納手段16にセキュリティレベルを問い合わせる。セキュリティレベル格納手段16は、自身が格納しているセキュリティレベルを暗号化／復号手段選択手段17に伝える。

【0044】暗号化／復号手段選択手段17は、セキュリティレベル格納手段16から知らされたセキュリティ

レベルに従って、暗号化／復号手段14-1～14-mの中から適切な暗号化／復号手段を選択し、その暗号化／復号手段を用いて乱数 R_{s2} と乱数 R_u の暗号化を行い、認証手段13に渡す。

【0045】認証手段13は得られた $E(K_{su}, R_{s2} \parallel R_u)$ をメッセージM5として、通信手段11を介してサーバ2に送る。

【0046】サーバ2は、送られてきたメッセージM5をセッション鍵 K_{us} で復号し、乱数 R_u 、 R_{s2} を取得する。取得した乱数 R_{s2} とメッセージM4で送った乱数とを照合し、一致すればメッセージM5を正しい端末装置1からの応答であると判断する。

【0047】

【発明の効果】以上説明したように、請求項1の発明によれば、利用者の認証に伴って該利用者の秘密鍵を用いた暗号／復号化処理を行う際、複数の暗号化／復号手段から暗号化／復号手段選択手段により、セキュリティレベル格納手段に格納された利用者や端末装置毎のセキュリティレベルに対応した暗号化／復号手段を選択することができ、利用者や端末装置毎のセキュリティレベルに応じた利用者の認証を行うことができ、コスト、端末装置の性能や設置場所等の利用者や端末装置側の条件に応じた最適のセキュリティを実現することができる。

【0048】また、請求項2の発明によれば、利用者の認証に伴って該利用者の秘密鍵を取得する際、複数の鍵管理手段から鍵管理手段選択手段により、セキュリティレベル格納手段に格納された利用者や端末装置毎のセキュリティレベルに対応した鍵管理手段を選択することができ、利用者や端末装置毎のセキュリティレベルに応じた利用者の認証を行うことができ、コスト、端末装置の性能や設置場所、ICカード装置の有無等の利用者や端末装置側の条件に応じた最適のセキュリティを実現することができる。

【図面の簡単な説明】

【図1】クライアントサーバ型分散ネットワークシステムの概要を示す構成図

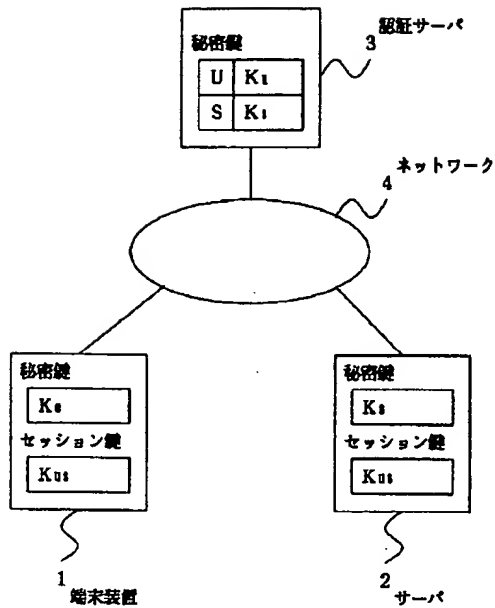
【図2】本発明方式を適用した端末装置の一実施例を示す構成図

【図3】端末装置、サーバ及び認証サーバ間でやりとりされるメッセージのシーケンスを示す図

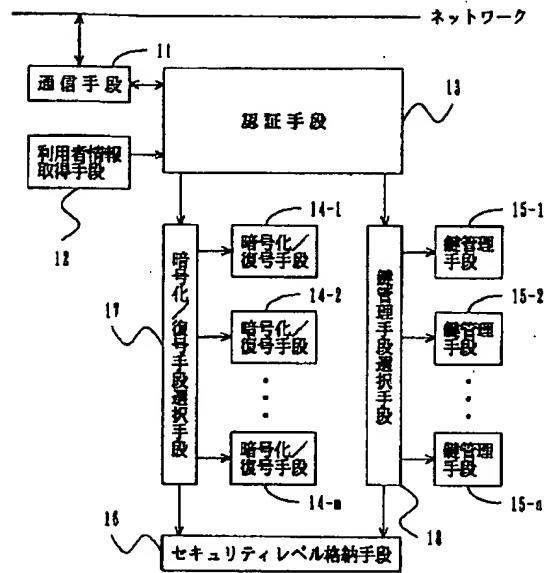
【符号の説明】

1…端末装置、2…サーバ、3…認証サーバ、4…ネットワーク、11…通信手段、12…利用者情報取得手段、13…認証手段、14-1～14-m…暗号化／復号手段、15-1～15-n…鍵管理手段、16…セキュリティレベル格納手段、17…暗号化／復号手段選択手段、18…鍵管理手段選択手段。

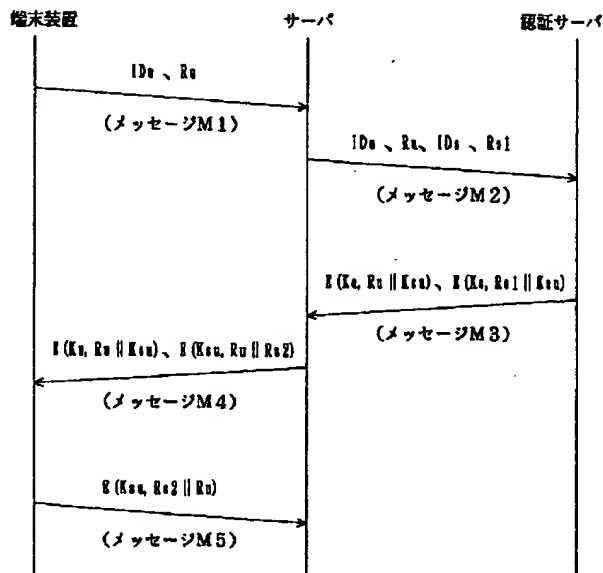
【図 1】



【図 2】



【図 3】



フロントページの続き

(51) Int. Cl. ⁶

H 0 4 L 9/12

// G 0 6 F 1/00

識別記号

庁内整理番号

F I

技術表示箇所

3 7 0